

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-040031

(43)Date of publication of application : 08.02.2000

(51)Int.Cl.

G06F 12/14

G09C 1/00

(21)Application number : 11-128382

(71)Applicant : HITACHI LTD

(22)Date of filing : 13.03.1990

(72)Inventor : NOZAWA MASASHI

SHIMADA AKINOBU

NISHIMURA TOSHIFUMI

TSUNOSE KATSUJI

TSUKIYAMA TOKUHIRO

YADA KIYOSHI

ISHII YASUHIRO

TAKARAGI KAZUO

HISAYOSHI YASUSHI

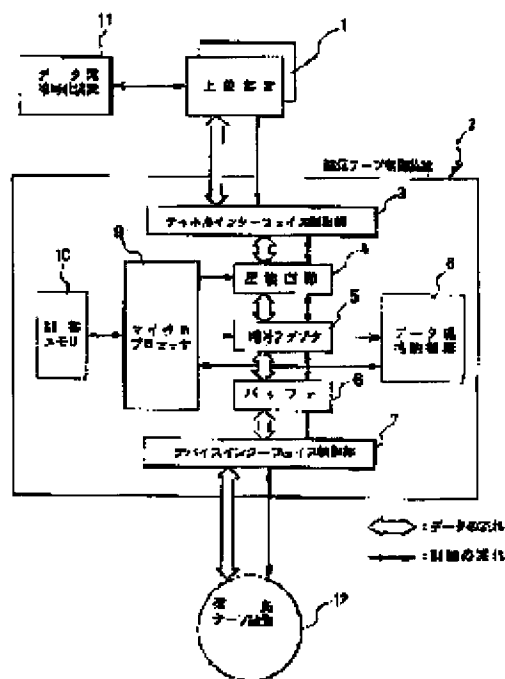
FUJITA FUJIO

(54) FILE ENCIPHERING METHOD AND INFORMATION PROCESSING SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To ensure the confidentiality of data exchanged between a host device and an external storage device without damaging the throughput of an information processing system.

SOLUTION: This information processing system makes a magnetic tape controller 2 exist between a host device 1 and a magnetic tape unit 12, connects a data key enciphering device 11 with the device 1, also connects the controller 2 with a data key storage mechanism 8. When data are written to the unit 12, it sets a raw data key to the mechanism 8, enciphers write data at an encryption adapter 5 and writes it on a magnetic tape after enciphering the raw data key produced by the device 1 by means of the device 11 and writing it in a



magnetic tape header. At the time of reading out, an enciphered data key of the magnetic tape header is read, decoded by the device 11 and set to the mechanism 8. The adapter 5 decodes read data and transfers it to the device 1.

(51)Int.Cl. ⁷	識別記号	F I	テマコード* (参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 B
G 0 9 C 1/00	6 6 0	G 0 9 C 1/00	6 6 0 D

審査請求 有 請求項の数 6 O L (全 11 頁)

(21)出願番号 特願平11-128382
 (62)分割の表示 特願平2-61917の分割
 (22)出願日 平成2年3月13日(1990.3.13)

(71)出願人 000005108
 株式会社日立製作所
 東京都千代田区神田駿河台四丁目6番地
 (72)発明者 野沢 正史
 神奈川県小田原市国府津2880番地 株式会
 社日立製作所小田原工場内
 (72)発明者 島田 朗伸
 神奈川県小田原市国府津2880番地 株式会
 社日立製作所小田原工場内
 (74)代理人 100080001
 弁理士 筒井 大和

最終頁に続く

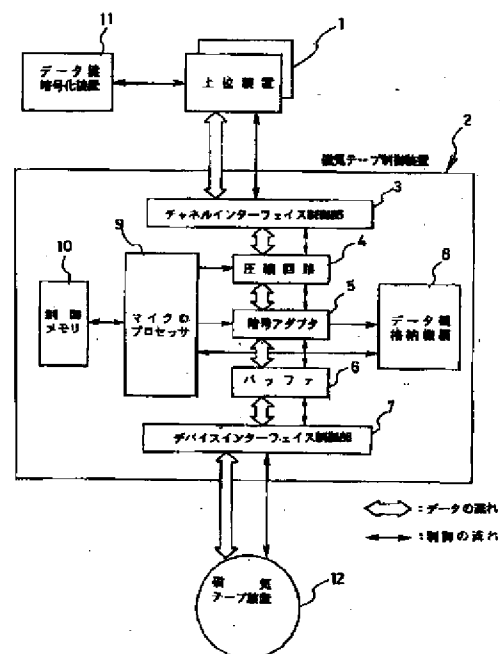
(54)【発明の名称】 ファイル暗号化方法および情報処理システム

(57)【要約】

【課題】 情報処理システムのスループットを損なうことなく、上位装置と外部記憶装置との間で授受されるデータの機密性の確保を実現する。

【解決手段】 上位装置1と、磁気テープ装置12との間に磁気テープ制御装置2を介在させた情報処理システムにおいて、上位装置1にデータ鍵暗号化装置11を接続するとともに、磁気テープ制御装置2にはデータ鍵格納機構8を備え、磁気テープ装置12へのデータ書き込み時には、上位装置1で生成した生データ鍵をデータ鍵暗号化装置11で暗号化して磁気テープヘッドに書き込んだ後、生データ鍵をデータ鍵格納機構8に設定し暗号アダプタ5にて書き込みデータを暗号化して磁気テープに書き込み、読み出し時には、磁気テープヘッドの暗号化されたデータ鍵を読み出しデータ鍵暗号化装置11で復号化してデータ鍵格納機構8に設定し暗号アダプタ5にて読み出しデータを復号化して上位装置1に転送する。

図 1



【特許請求の範囲】

【請求項1】 上位装置、

前記上位装置に接続された鍵暗号化装置、
 前記上位装置との間でデータの授受を行う外部記憶装置、並びに、
 前記上位装置及び前記外部記憶装置の間に介在してデータの授受を制御する外部記憶装置の制御装置とからなる情報処理システムにおけるファイル暗号化方法であって、
 前記鍵暗号化装置から暗号化された鍵を出力する第1のステップ、
 前記暗号化された鍵を前記外部記憶装置の制御装置が受け取る第2のステップ、及び、
 前記制御装置において、前記上位装置からのデータに対し、前記暗号化される前の鍵を用いて暗号化を行う第3のステップを有するファイル暗号化方法。

【請求項2】 請求項1記載のファイル暗号化方法において、更に、
 前記暗号化された鍵及び前記暗号化されたデータを前記外部記憶装置の記憶媒体に格納する第4のステップを有するファイル暗号化方法。

【請求項3】 上位装置、
 前記上位装置に接続され、暗号を解読するための鍵を暗号化して出力する機能を有する暗号化装置、
 前記上位装置との間でデータの授受を行う外部記憶装置、並びに、
 前記上位装置および前記外部記憶装置の間に介在してデータの授受を制御する機能と、
 前記上位装置から、暗号化された鍵と暗号化される前の鍵を受け取り、前記上位装置からのデータに対し、前記暗号化される前の鍵を用いて暗号化を行う機能とを有する制御装置とからなる情報処理システム。

【請求項4】 請求項3記載の情報処理システムにおいて、更に、前記制御装置は、
 前記暗号化された鍵及び前記暗号化されたデータを、前記外部記憶装置に格納する機能を有する情報処理システム。

【請求項5】 上位装置、
 前記上位装置に接続された鍵暗号化装置、
 前記上位装置との間でデータの授受を行う外部記憶装置、並びに、
 前記上位装置及び前記外部記憶装置の間に介在してデータの授受を制御する外部記憶装置の制御装置とからなる情報処理システムにおけるファイル暗号化方法であって、
 前記外部記憶装置の記憶媒体に格納された、暗号化された鍵を読み出す第1のステップ、
 前記暗号化装置において、前記暗号化された鍵から暗号化される前の鍵を復元する第2のステップ、
 前記暗号化される前の鍵を前記制御装置に格納する第3

のステップ、及び、

前記制御装置において、前記外部記憶装置からのデータに対し、前記暗号化される前の鍵を用いてデータの復号化を行う第4のステップを有するファイル暗号化方法。

【請求項6】 上位装置、

前記上位装置に接続され、暗号化された鍵を復元して暗号化される前の鍵を出力する機能を有する暗号化装置、
 前記上位装置との間でデータの授受を行う外部記憶装置、並びに、
 前記上位装置及び前記外部記憶装置の間に介在してデータの授受を制御する機能と、
 前記外部記憶装置に格納された暗号化された鍵を読み出す機能と、
 前記暗号化装置から復元した暗号化される前の鍵を受け取り、前記外部記憶装置からのデータに対し、該暗号化される前の鍵を用いて復号化を行う機能とを有する制御装置を有する情報処理システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ファイル暗号技術に関し、特に、コンピュータシステムの外部記憶装置におけるデータファイルなどの機密保持に好適な技術に関する。

【0002】

【従来の技術】近年、コンピュータシステムの急速な大形化およびネットワーク化などに伴い、一つのシステムに対して非常に多数の人間がアクセスを行う機会が増えたことから、機密データの確実な保護管理を要請する声が高まり、この分野の重要な技術課題となっている。

【0003】このような背景の中で、大量のデータの記録・再生を行うコンピュータシステムの外部記憶装置についても、データファイルの暗号化による機密保持技術が考案されている。

【0004】たとえば、特開昭54-87032号公報には、チャネルなどの上位システムに接続された暗号装置によって、データの暗号化および復号化を行う技術が開示されている。

【0005】すなわち、当該技術においては、通常のデータを、上位システムの暗号装置に送り、ここで鍵を用いる所定のアルゴリズムによって、全く意味を持たないデータに暗号化した後に外部記憶装置に送出して記憶媒体に書き込ませ、データの読み出しに際しては逆の手順で、上位システム側においてデータの復号化を行うようにしている。

【0006】また、データの暗号化、復号化処理を鍵を用いて制御するアルゴリズムとしては、たとえば、特開昭52-130505号公報に開示されるものが知られている。

【0007】また、この鍵を受け渡すことにより、当該システムにおいて作成した暗号化データが記録された媒

体を他のシステムに運搬し、そこで暗号化データの読み出しおよび復元を行うことができる。

【0008】

【発明が解決しようとする課題】ところが、上述の前者の従来技術では、外部記憶装置にデータを書き込む場合には、一旦チャンネルに接続されている暗号化装置に送出して暗号化し、暗号化後に、再び暗号化されたデータを暗号化装置から読み出し、チャンネルを介して暗号化されたデータを外部記憶装置に書き込むという手順を踏むため、チャンネルおよびこれに接続された暗号化装置の部分

10

がデータの入出力処理の隘路となり、チャンネルと当該チャンネルに接続されている種々の外部記憶装置との間における単位時間当たりのデータ転送能力（スループット）などの性能が低下するという問題がある。

【0009】さらに、上述の後者の従来技術に示されているように、鍵を用いて制御を行うアルゴリズムによってデータの暗号化を行う場合には、暗号化されたデータは、当該鍵の内容を知ることができるならば誰でも、また、特定のシステムならばどのシステムでもこれを復号化して読むことができる。すなわち、鍵を用いるアルゴリズムによって暗号化されたデータの機密性は、ひとえに鍵の管理にかかっているといえる。従って、当該鍵をより複雑な形の暗号に変換するなどして厳重に管理することは、鍵を用いたデータの暗号化ファイルシステムの高い機密性を確保する上で必須条件である。

20

【0010】そこで、本発明の目的は、情報処理システムにおいてシステムのスループットを損なうことなく、上位装置と外部記憶装置との間で授受されるデータの機密性の確保を実現することが可能なファイル暗号化方法を提供することにある。

30

【0011】本発明の他の目的は、システムのスループットを損なうことなく、上位装置と外部記憶装置との間で授受されるデータの機密性の確保を実現することが可能な情報処理システムを提供することにある。

【0012】本発明の他の目的は、データの暗号化のアルゴリズムを制御する鍵の機密保持を確実にして、システム全体の機密保持性能を高めることが可能な情報処理システムを提供することにある。

【0013】本発明の他の目的は、データ圧縮による外部記憶装置の効率的な利用と暗号化によるデータの機密性の確保とを両立させることが可能な情報処理システムを提供することにある。

40

【0014】本発明の他の目的は、データ鍵と当該データ鍵によって暗号化されたデータの管理を安全かつ容易に行うことが可能な情報処理システムを提供することにある。

【0015】本発明の前記ならびにその他の目的と新規な特徴は、本明細書の記述および添付図面から明らかになるであろう。

【0016】

【課題を解決するための手段】本願において開示される発明のうち、代表的なものの概要を簡単に説明すれば、下記のとおりである。

【0017】すなわち、本発明になるファイル暗号化方法は、上位装置、前記上位装置に接続された鍵暗号化装置、前記上位装置との間でデータの授受を行う外部記憶装置、並びに、前記上位装置及び前記外部記憶装置の間に介在してデータの授受を制御する外部記憶装置の制御装置とからなる情報処理システムにおけるファイル暗号化方法であって、前記鍵暗号化装置から暗号化された鍵を出力する第1のステップ、前記暗号化された鍵を前記外部記憶装置の制御装置が受け取る第2のステップ、及び、前記制御装置において、前記上位装置からのデータに対し、前記暗号化される前の鍵を用いて暗号化を行う第3のステップを有するものである。

【0018】また、本発明のファイル暗号化方法は、上述のファイル暗号化方法において、更に、前記暗号化された鍵及び前記暗号化されたデータを前記外部記憶装置の記憶媒体に格納する第4のステップを有するものである。

【0019】また、本発明の情報処理システムは、上位装置、前記上位装置に接続され、暗号を解読するための鍵を暗号化して出力する機能を有する暗号化装置、前記上位装置との間でデータの授受を行う外部記憶装置、並びに、前記上位装置および前記外部記憶装置の間に介在してデータの授受を制御する機能と、前記上位装置から、暗号化された鍵と暗号化される前の鍵を受け取り、前記上位装置からのデータに対し、前記暗号化される前の鍵を用いて暗号化を行う機能とを有する制御装置とからなるものである。

【0020】また、本発明の情報処理システムは、上述の情報処理システムにおいて、更に、前記制御装置は、前記暗号化された鍵及び前記暗号化されたデータを、前記外部記憶装置に格納する機能を有するものである。

【0021】本発明になるファイル暗号化方法は、上位装置、前記上位装置に接続された鍵暗号化装置、前記上位装置との間でデータの授受を行う外部記憶装置、並びに、前記上位装置及び前記外部記憶装置の間に介在してデータの授受を制御する外部記憶装置の制御装置とからなる情報処理システムにおけるファイル暗号化方法であって、前記外部記憶装置の記憶媒体に格納された、暗号化された鍵を読み出す第1のステップ、前記暗号化装置において、前記暗号化された鍵から暗号化される前の鍵を復元する第2のステップ、前記暗号化される前の鍵を前記制御装置に格納する第3のステップ、及び、前記制御装置において、前記外部記憶装置からのデータに対し、前記暗号化される前の鍵を用いてデータの復号化を行う第4のステップを有するものである。

【0022】また、本発明の情報処理システムは、上位装置、前記上位装置に接続され、暗号化された鍵を復元

50

して暗号化される前の鍵を出力する機能を有する暗号化装置、前記上位装置との間でデータの授受を行う外部記憶装置、並びに、前記上位装置及び前記外部記憶装置の間に介在してデータの授受を制御する機能と、前記外部記憶装置に格納された暗号化された鍵を読み出す機能と、前記暗号化装置から復元した暗号化される前の鍵を受け取り、前記外部記憶装置からのデータに対し、該暗号化される前の鍵を用いて復号化を行う機能とを有する制御装置を有するものである。

【0023】上記した本発明のファイル暗号化方法によれば、通常のデータの暗号化や復号化などの煩雑な処理に上位装置が関与しないので、データの暗号化や復号化に伴う上位装置の負担が大幅に軽減され、システム全体のスループットを損なうことなく、外部記憶装置に格納されるデータの機密性を確保することができる。

【0024】また、上記した本発明の情報処理システムによれば、たとえば、外部記憶装置に設けられた暗号化機能および復号化機能において、所望の生データ鍵によって制御されるアルゴリズムにより、上位装置との間で授受されるデータの暗号化および復号化を行わせるとともに、外部記憶装置が用いる生データ鍵の暗号化および復号化を上位装置に接続されている暗号化装置において行わせることにより、通常のデータの暗号化や復号化などの煩雑な処理に上位装置が関与する必要がなくなり、データの暗号化や復号化に伴う上位装置の負担が大幅に軽減され、システム全体のスループットを損なうことなく、外部記憶装置に格納されるデータの機密性を確保することができる。

【0025】また、データの暗号化や復号化に用いられ、データの機密保持性能を左右する生データ鍵を、暗号化装置によってより高度で複雑な暗号に変換することにより、安全かつ確実に保管することができるので、システム全体の機密保持性能を高めることができる。

【0026】また、一般に暗号化によってデータの冗長性は失われるが、本発明の場合には、外部記憶装置において、上位装置から到来するデータの暗号化に先立って、圧縮処理を施すことにより、通常の暗号化を行わない場合と同様に、効果的なデータ圧縮によって大幅なデータ量の削減を実現することができ、データ圧縮による外部記憶装置の効率的な利用と暗号化によるデータの機密性の確保とを両立させることができる。

【0027】また、上位装置の側の暗号装置においてデータ鍵を複雑に暗号化することにより、データ鍵を当該データ鍵に基づいて外部記憶装置において暗号化された通常のデータと共に同一の記録媒体上に安全に格納することができ、データ鍵と当該データ鍵によって暗号化されたデータの管理を安全かつ容易に行うことが可能となる。

【0028】

【発明の実施の形態】以下、本発明の一実施の形態であ

るファイル暗号化方法および情報処理システムの一例について、図面を参照しながら詳細に説明する。

【0029】図1は、本実施の形態における情報処理システムの構成の一例を示すブロック図であり、図2および図3は、本実施の形態のファイル暗号化方法および情報処理システムの作用の一例を説明する説明図である。

【0030】まず、図1を参照しながら、本実施の形態の情報処理システムの構成を説明する。

【0031】なお、以下の説明では、情報処理システムを構成する外部記憶装置の一例として磁気テープサブシステムの場合について説明する。

【0032】たとえば、コンピュータシステムなどの情報処理システムにおける中央処理装置などからなる上位装置1には、当該上位装置1に代わって外部とのデータの入出力を制御する動作を行う図示しないチャネルなどが設けられており、このチャネルには、磁気テープ制御装置2を介して磁気テープ装置12が接続されている。

【0033】磁気テープ制御装置2は、上位装置1と磁気テープ装置12との間における情報の授受を制御する働きをするとともに、磁気テープ装置12は、図示しない磁気テープなどの記憶媒体に対する実際の情報の記録／再生動作を行うようになっている。

【0034】この場合、上位装置1には、図示しないチャネルを介して、後述のような動作を行うデータ鍵暗号化装置11が接続されている。

【0035】磁気テープ制御装置2は、制御メモリ10に格納されているプログラムによって全体の制御を行うマイクロプロセッサ9と、このマイクロプロセッサ9の配下で上位装置1の側との情報の授受を制御するチャネルインターフェイス制御部3、および磁気テープ装置12の側との間における情報の授受を制御するデバイスインターフェイス制御部7とを備えている。

【0036】さらに、チャネルインターフェイス制御部3とデバイスインターフェイス制御部7との間には、必要に応じて、上位装置1と磁気テープ装置12との間で授受されるデータの圧縮／伸張処理などを行う圧縮回路4と、当該データが一時的に保持されるバッファ6とが順に設けられている。

【0037】このバッファ6は、たとえば半導体メモリなどからなり、動作の高速な上位装置1と、比較的動作の遅い磁気テープ装置12との間に介在して周知の記憶階層を構成し、両者間で授受されるデータを一時的に記憶することにより、上位装置1と磁気テープ装置12との間における動作速度の大きな隔たりを吸収して、両者間におけるデータ転送の効率化を図る働きをしている。

【0038】この場合、チャネルインターフェイス制御部3の側の圧縮回路4とデバイスインターフェイス制御部7の側のバッファ6との間には、暗号アダプタ5と、この暗号アダプタ5によってアクセスされるデータ鍵格納機構8とが設けられている。

【0039】この暗号アダプタ5は、たとえば、上位装置1の側からデータ鍵格納機構8に後述のようにして設定される生データ鍵によって制御される所望のアルゴリズムにより、上位装置1と磁気テープ装置12との間で授受されるデータの暗号化および復号化を行うようになっている。

【0040】すなわち、本実施の形態の場合には、上位装置1から磁気テープ装置12に格納すべく到来するデータは、必要に応じて、一旦、圧縮回路4において圧縮処理が施された後、暗号アダプタ5において暗号化され、バッファ6およびデバイスインターフェイス制御部7を経て磁気テープ装置12に書き込まれる。

【0041】また逆に、磁気テープ装置12に格納されている暗号化されたデータの読み出しに際しては、目的のデータがデバイスインターフェイス制御部7を介して当該磁気テープ装置12からバッファ6に読み出され、この読み出された暗号状態のデータを暗号アダプタ5において復号化した後、さらに、必要に応じて圧縮回路4において伸張処理を施し、チャンネルインターフェイス制御部3を介して上位装置1に送出される。

【0042】以下、図2および図3などを参照しながら、本実施の形態の情報処理システムの動作の一例を説明する。

【0043】まず、上位装置1から送出されるデータの磁気テープ装置12への書き込み動作の一例について説明する。

【0044】上位装置1は、まず、下位の磁気テープ装置12との間で授受されるデータの、磁気テープ制御装置2における暗号化／復号化に必要な生データ鍵を生成し、これを付属のデータ鍵暗号化装置11に与え、暗号化を指示する。

【0045】なお、この生データ鍵の生成は、上位装置1において行うことに限らず、当該上位装置1からの指示に従って、データ鍵暗号化装置11の内部で行ってもよいことはいうまでもない。

【0046】データ鍵暗号化装置11は、これを受けて生データ鍵の複雑かつ高度の暗号化を行い暗号化データ鍵を生成する。

【0047】次に、上位装置1は、図示しないチャンネルなどを介してデータ鍵暗号化装置11から暗号化された暗号化データ鍵を読み出し、磁気テープ制御装置2を介して、磁気テープ装置12に装填されている図示しない磁気テープ媒体における通常のデータ記録領域以前のヘッダ部などに、当該暗号化データ鍵を書き込むように指示する。

【0048】また、上位装置1は、生データ鍵を磁気テープ制御装置2に送出するとともに、当該磁気テープ制御装置2のマイクロプロセッサ9に対して、当該生データ鍵をデータ鍵格納機構8に設定するように指示する。

【0049】なお、特に限定されないが、データ鍵暗号

化装置11においては、磁気テープ制御装置2に設定すべき生データ鍵の生成および送出に際して、当該生データ鍵を、磁気テープ制御装置2の暗号アダプタ5において解読可能な程度に暗号化し、磁気テープ制御装置2において完全な生データ鍵に復号化してデータ鍵格納機構8に設定するようにしてもよい。

【0050】これを受けて、磁気テープ制御装置2がデータ鍵格納機構8に生データ鍵を設定した後、上位装置1は、書き込みデータを図示しないチャンネルを介して磁気テープ制御装置2のチャンネルインターフェイス制御部3に送出する。

【0051】そして、たとえばデータ圧縮を行う場合には、チャンネルインターフェイス制御部3に到来するデータは、マイクロプロセッサ9の指示により、まず圧縮回路4に送られて所望のアルゴリズムによる圧縮処理が施される。

【0052】その後、マイクロプロセッサ9の指示により、圧縮済みのデータは暗号アダプタ5に送り込まれ、当該暗号アダプタ5は、前述のようにしてデータ鍵格納機構8に設定されている生データ鍵によって制御される所望のアルゴリズムによってデータの暗号化を行う。

【0053】こうして、圧縮処理および暗号化が順に施されたデータは、バッファ6およびデバイスインターフェイス制御部7を経て磁気テープ装置12に装填されている図示しない磁気テープ媒体に順次書き込まれる。

【0054】そして、所定の書き込み処理の終了後、上位装置1は、磁気テープ制御装置2に対して、生データ鍵のリセットを指示し、これを受けた当該磁気テープ制御装置2のマイクロプロセッサ9は、データ鍵格納機構8に設定されている生データ鍵の消去処理を行う。

【0055】このような、データの書き込み処理における上位装置1、データ鍵暗号化装置11、磁気テープ制御装置2の各々の一連の動作の一例を相互に関連付けて示したものが図2である。

【0056】一方、暗号化されて磁気テープ装置12の磁気テープ媒体に格納されているデータの上位装置1による読み出し動作の一例を示せば次のようになる。

【0057】まず、上位装置1は、磁気テープ制御装置2に対して、磁気テープ装置12に装填されている磁気テープ媒体において、前述のようにして暗号化された暗号化データ鍵が格納されているヘッダ部の読み取りを指示する。

【0058】これを受けて磁気テープ制御装置2のマイクロプロセッサ9は、磁気テープ装置12の当該磁気テープ媒体から、以前の記録時などに前述のようにして当該媒体に書き込まれている暗号化データ鍵を読み込む。

【0059】次に、上位装置1は、磁気テープ制御装置2に読み込まれた暗号化データ鍵を、チャンネルを介してデータ鍵暗号化装置11に送り、暗号化データ鍵を復号化して生データ鍵を生成するように指示する。

【0060】これを受けて、データ鍵暗号化装置11は、暗号化データ鍵に復号化処理を施して生データ鍵を生成する動作を行う。

【0061】こうして得られた生データ鍵は、上位装置1の指示により、図示しないチャンネルを介して、再び磁気テープ制御装置2に送出され、当該磁気テープ制御装置2は、データ鍵格納機構8にこの生データ鍵を設定する。

【0062】なお、特に限定されないが、データ鍵暗号化装置11においては、暗号化データ鍵からの磁気テープ制御装置2に設定すべき生データ鍵の復号化を、磁気テープ制御装置2の暗号アダプタ5において解読可能な程度の暗号化状態に止め、磁気テープ制御装置2において完全な生データ鍵に復号化してデータ鍵格納機構8に設定するようにしてもよい。

【0063】次に、上位装置1は、磁気テープ制御装置2に対して、磁気テープ装置12に装填されている磁気テープ媒体上に前述のようにして暗号化されて記録されているデータの読み込みを指示する。

【0064】これを受けた磁気テープ制御装置2のマイクロプロセッサ9は、デバイスインターフェイス制御部7にデータの読み出しを指示する。

【0065】そして、磁気テープ装置12から読み出されたデータは、一旦バッファ6に格納され、その後、暗号アダプタ5は、暗号化されているデータを当該バッファ6から読み出し、データ鍵格納機構8に設定されている生データ鍵によって制御されるアルゴリズムによって復号化を行う。

【0066】その後、こうして復号化されたデータが、たとえば記録時に圧縮処理が施されたデータの場合には、マイクロプロセッサ9は、復号化された当該データを圧縮回路4に通し、伸張処理を施して非圧縮データに戻す。

【0067】そして、復元されたデータは上位装置1の指示により、チャンネルインターフェイス制御部3を介して上位装置1の側に送出される。

【0068】こうした、上位装置1による磁気テープ装置12の磁気テープ媒体からの一連のデータの読み込み処理が完了すると、上位装置1の指示により、磁気テープ制御装置2は、当該磁気テープ制御装置2のデータ鍵格納機構8に設定されている生データ鍵をリセットして消去する。

【0069】このような、磁気テープ装置12からのデータの読み込み処理における上位装置1、データ鍵暗号化装置11、磁気テープ制御装置2の各々の一連の動作の一例を相互に関連付けて示したものが図3である。

【0070】以上説明したように、本実施の形態のファイル暗号化方法および情報処理システムによれば、磁気テープ装置12の磁気テープ記憶媒体に対して記録／再生されるデータの暗号化を、磁気テープ制御装置2に備

えられた暗号アダプタ5およびデータ鍵格納機構8により、当該データ鍵格納機構8に設定された生データ鍵に制御される所望のアルゴリズムによって行うようにしたので、通常のデータの暗号化／復号化の煩雑な処理に上位装置1が関与する必要がなく、データの機密保持に伴う上位装置1の負荷の増大を抑止することができる。

【0071】この結果、上位装置1におけるスループットなどの性能を損なうことなくシステムにおけるデータの高度の機密保持を実現することができる。

【0072】また、磁気テープ制御装置2におけるデータの暗号化／復号化の制御に用いられる生データ鍵の暗号化／復号化を、上位装置1に接続されたデータ鍵暗号化装置11において独立に行うので、上位装置1などにおけるスループットの低下などを懸念することなく、データの機密保持に重要な生データ鍵に対して、通常のデータよりも複雑かつ高度の暗号化処理を施して厳重に管理することが可能となり、高い機密保持性能を有する情報処理システムを実現することができる。

【0073】さらに、磁気テープ制御装置2においては、データの暗号化に先立って、必要に応じてデータ圧縮処理を行うので、暗号化によってデータが冗長性を失う前に、通常の場合と同様の高い圧縮率でデータを圧縮することが可能となり、データ圧縮による磁気テープ装置12に装填された磁気テープ媒体の効率的な利用と暗号化によるデータの高い機密性の確保とを両立させることができる。

【0074】また、データ鍵暗号化装置11による生データ鍵の複雑な暗号化により、暗号化されたデータ鍵と、当該データ鍵に基づいて磁気テープ制御装置2において暗号化された通常のデータとを、同一の記録媒体に安全に格納することができる。

【0075】この結果、たとえば、長期間にわたって大量のデータを暗号化して保管する場合や、特定の複数の情報処理施設の間で暗号化されたデータを相互に受け渡して使用する場合などに、データ鍵の管理を安全かつ容易に行うことが可能になる。

【0076】以上本発明者によってなされた発明を実施の形態に基づき具体的に説明したが、本発明は前記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることはいうまでもない。

【0077】たとえば、上記の説明では、情報処理システムを構成する外部記憶装置の一例として、磁気テープサブシステムの場合について説明したが、これに限らず、他の外部記憶装置でもよい。

【0078】また、データの暗号化／復号化を行う磁気テープサブシステムの構成としては、前記実施の形態に例示したものに限らず、同様の機能を実現できるものであれば他の構成であってもよいことはいうまでもない。

【0079】

【発明の効果】本願において開示される発明のうち、代

表的なものによって得られる効果を簡単に説明すれば、以下のとおりである。

【0080】すなわち、本発明のファイル暗号化方法によれば、情報処理システムにおいてシステムのスループットを損なうことなく、上位装置と外部記憶装置との間で授受されるデータの機密性の確保を実現することができる、という効果が得られる。

【0081】また、本発明の情報処理システムによれば、システムのスループットを損なうことなく、上位装置と外部記憶装置との間で授受されるデータの機密性の確保を実現することができる、という効果が得られる。

【0082】また、本発明の情報処理システムによれば、データの暗号化のアルゴリズムを制御する鍵の機密保持を確実にして、システム全体の機密保持性能を高めることができる、という効果が得られる。

【0083】また、本発明の情報処理システムによれば、データ圧縮による外部記憶装置の効率的な利用と暗号化によるデータの機密性の確保とを両立させることができる、という効果が得られる。

【0084】また、本発明の情報処理システムによれば、

ば、データ鍵と当該データ鍵によって暗号化されたデータの管理を安全かつ容易に行うことができる、という効果が得られる。

【図面の簡単な説明】

【図1】本発明の一実施の形態である情報処理システムの構成の一例を示すブロック図である。

【図2】本発明の一実施の形態であるファイル暗号化方法および情報処理システムの作用の一例を示す説明図である。

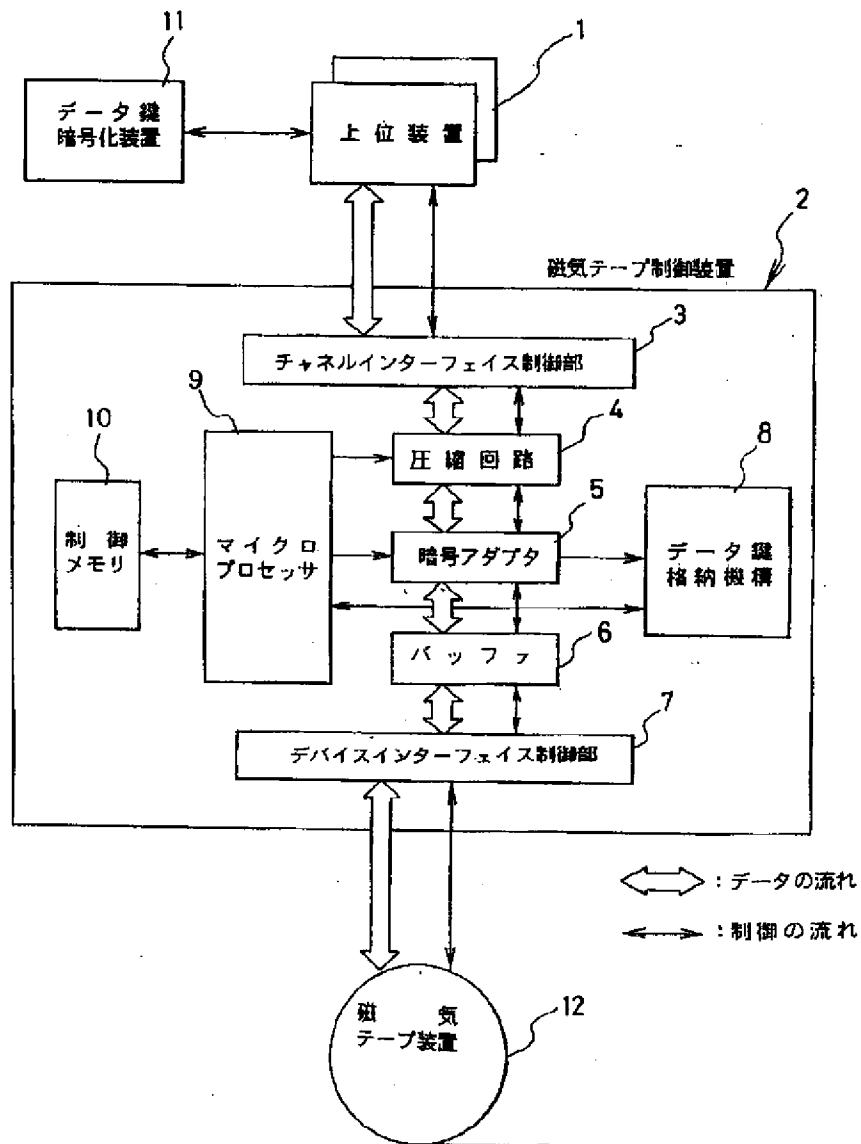
【図3】本発明の一実施の形態であるファイル暗号化方法および情報処理システムの作用の一例を示す説明図である。

【符号の説明】

1・・・上位装置、2・・・磁気テープ制御装置、3・・・チャンネルインターフェイス制御部、4・・・圧縮回路、5・・・暗号アダプタ、6・・・バッファ、7・・・デバイスインターフェイス制御部、8・・・データ鍵格納機構、9・・・マイクロプロセッサ、10・・・制御メモリ、11・・・データ鍵暗号化装置、12・・・磁気テープ装置。

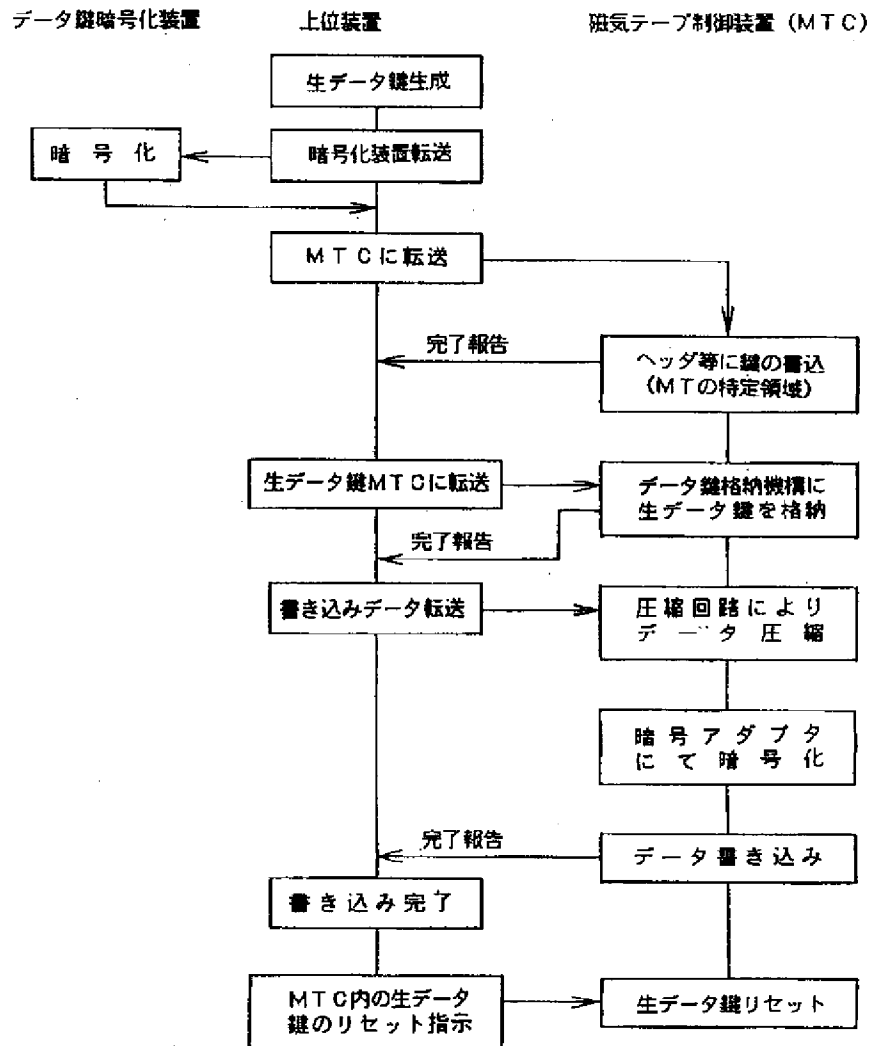
【図1】

図 1



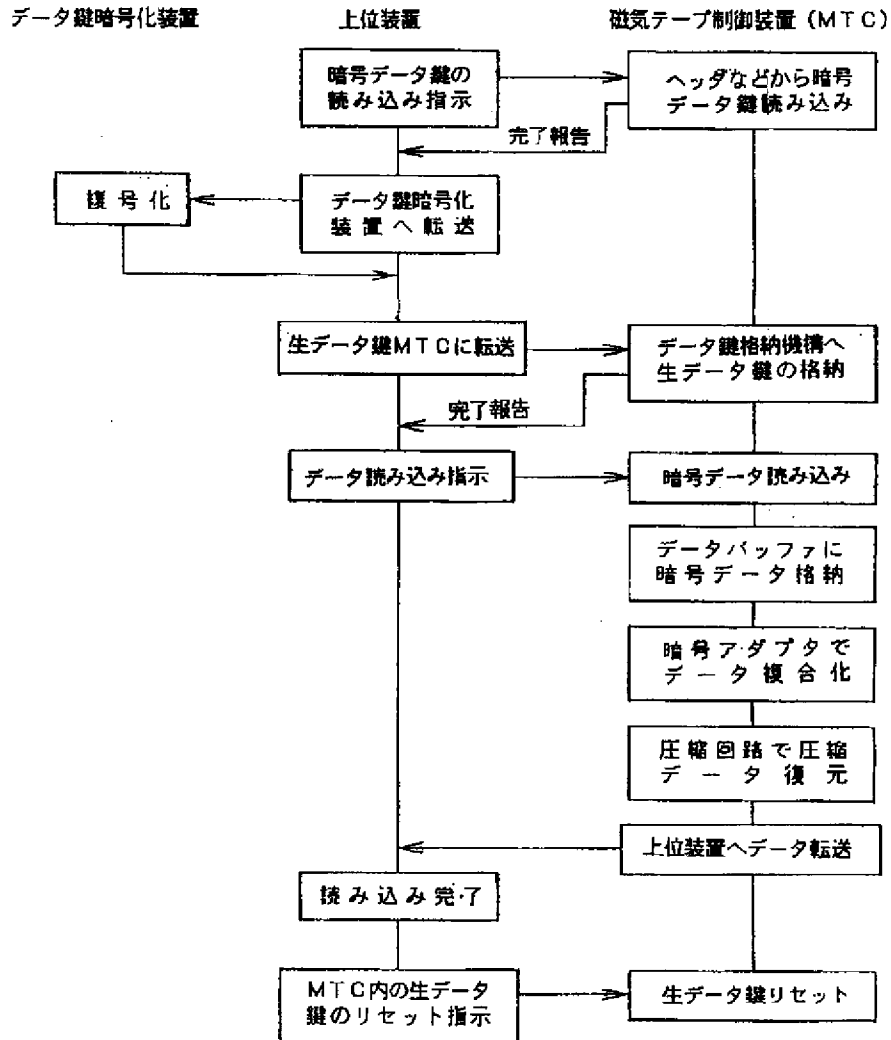
【図2】

図 2



【図3】

図 3



フロントページの続き

(72)発明者 西村 利文
 神奈川県小田原市国府津2880番地 株式会
 社日立製作所小田原工場内

(72)発明者 角瀬 勝治
 神奈川県小田原市国府津2880番地 株式会
 社日立製作所小田原工場内

(72)発明者 築山 徳広
 神奈川県小田原市国府津2880番地 株式会
 社日立製作所小田原工場内

(72)発明者 矢田 潔
 神奈川県秦野市堀山下1番地 株式会社日
 立製作所神奈川工場内

(72)発明者 石井 保弘
 神奈川県秦野市堀山下1番地 株式会社日
 立製作所神奈川工場内

(72)発明者 宝木 和夫
 神奈川県川崎市麻生区王禅寺1099番地 株
 式会社日立製作所システム開発研究所内

(72)発明者 久芳 靖
神奈川県横浜市戸塚区戸塚町5030番地 株
式会社日立製作所ソフトウェア工場内

(72)発明者 藤田 不二男
神奈川県横浜市戸塚区戸塚町5030番地 株
式会社日立製作所ソフトウェア工場内